Claims

What is claimed is:

1. A method comprising:

creating a data structure including a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key comprising a master key encrypted using a password associated with the one of the plurality of users; and

delivering the data structure to one or more of the plurality of users.

2. A method as recited in claim 1, wherein the act of delivering comprises delivering the data structure to each of the plurality of users.

3. A method as recited in claim 1, wherein each master key is encrypted using a hash of the password associated with the one of the plurality of users.

4. A method as recited in claim 1, wherein each master key is encrypted using a one-way hash of the password associated with the one of the plurality of users.

5. A method as recited in claim 1, wherein each master key is encrypted using a cryptographic hash of the password associated with the one of the plurality of users.

6. A method as recited in claim 1, wherein each user key has an integrity verification feature associated therewith.

7. A method as recited in claim 1, wherein each master key has an integrity verification feature associated therewith.

8. A method as recited in claim 1, wherein each master key and each master key has an integrity verification feature associated therewith.

9. A method as recited in claim 1, wherein each user key includes a checksum.

10. A method as recited in claim 1, wherein each user key includes a keyed-hash message authentication code.

11. A method as recited in claim 1, further comprising:

transforming data using the master key.

12. A method as recited in claim 1, further comprising:

storing data transformed using the master key; and

controlling access by the plurality of users to the transformed data.

13. A method as recited in claim 1, further comprising:

storing data transformed using the master key;

receiving a user id and user password from one of the plurality of users; and

controlling access to the transformed data by the one of the plurality of users based on the received user id and user password.

14. A method as recited in claim 1, further comprising:

storing data transformed using the master key;

receiving a user id and user password from one of the plurality of users; and

accessing the transformed data using the received user id and user password.

15. A method as recited in claim 1, further comprising:

storing data transformed using the master key;

receiving a user id and user password from one of the plurality of users;

selecting a user key from the data structure based on the received user id;

decrypting the selected user id using the received password to reproduce the master key; and

using the master key to access the data.

16. A method as recited in claim 1, further comprising:

storing data watermarked using the master key;

receiving a user id and user password from one of the plurality of users; and

selecting a user key from the data structure based on the received user id;

hashing the received password to produce a hash value;

decrypting the selected user id using the hash value to reproduce the master key; and

using the master key to access the watermarked data.

17. A method comprising:

retrieving a user key associated with a first user of a plurality of users from a data structure comprising a plurality of user keys, each user key comprising a master key encrypted using a password associated with a unique one of the plurality of users;

decrypting the retrieved user key using a password associated with the first user to produce a master key; and

accessing data using the master key.

18. A method as recited in claim 17, wherein the user key is retrieved using a user id associated with the first user.

19. A method as recited in claim 17, wherein the data structure comprises a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key associated with the one of the plurality of users.

20. A method as recited in claim 17, wherein the data structure comprises a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key associated with the one of the plurality of users, and wherein the user key is retrieved using a user id associated with the first user.

21. A method as recited in claim 17, wherein the act of decrypting the user key comprises decrypting the user key using a hash of the password associated with the first user.

22. A method as recited in claim 17, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user to produce a hash value; and

using the hash value as a decryption key to decrypt the user key.

23. A method as recited in claim 17, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user using a one-way hash function; and

using the result of the one-way hash function as a decryption key to decrypt the user key.

24. A method as recited in claim 17, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user using a cryptographic hash function; and

using the result of the cryptographic hash function as a decryption key to decrypt the user key.

25. A method as recited in claim 17, wherein each of the plurality of user keys includes a data verification feature.

26. A method as recited in claim 17, wherein each of the plurality of master keys includes a data verification feature.

27. A method as recited in claim 17, further comprising:

verifying the integrity of the retrieved user key.

28. A method as recited in claim 17, wherein the retrieved user key includes an integrity verification feature and wherein the method further comprises verifying the integrity of the retrieved user key using the integrity verification feature.

29. A method as recited in claim 17, wherein the retrieved user key includes a checksum and wherein the method further comprises verifying the integrity of the retrieved user key using the checksum.

30. A method as recited in claim 17, wherein the retrieved user key includes a message authentication code and wherein the method further comprises verifying the integrity of the retrieved user key using the message authentication code.

31. A method as recited in claim 17, wherein the retrieved user key includes a keyed-hash message authentication code and wherein the method further comprises verifying the integrity of the retrieved user key using the keyed-hash message authentication code.

32. A computer readable medium having stored thereon a data structure comprising:

a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key comprising a master key encrypted using a password associated with the one of the plurality of users.

33. A computer readable medium as recited in claim 32, wherein each user key comprises a master key encrypted using a hash of the password associated with the one of the plurality of users.

34. A computer readable medium as recited in claim 32, wherein each user key comprises a master key encrypted using a one-way hash of the password associated with the one of the plurality of users.

35. A computer readable medium as recited in claim 32, wherein each user key comprises a master key encrypted using a cryptographic hash of the password associated with the one of the plurality of users.

36. A computer readable medium as recited in claim 32, wherein each user key includes an integrity verification feature.

37. A computer readable medium as recited in claim 32, wherein each master key includes an integrity verification feature.

38. A computer readable medium as recited in claim 32, wherein each user key includes a checksum.

39. A computer readable medium as recited in claim 32, wherein each user key includes a keyed-hash message authentication code.

40. A system comprising:

a hashing module operable to hash each of a plurality of user passwords to produce a plurality of hash values;

an encryption module operable to create a plurality of user keys, each user key comprising a master key encrypted using one of the hash values as an encryption key; and

a data structure creation module operable to associate each of the user keys with a user id in a data structure.

41. A system as defined in claim 40, wherein the hashing module produces the hash values using a one-way hashing function.

42. A system as defined in claim 40, wherein the hashing module produces the hash values using a cryptographic hashing function.

43. A system as defined in claim 40, wherein the data structure creation module associates each user key with a user id in a user id-user key pair, and wherein each user id-user key pair is associated with a single user.

44. A system as defined in claim 40, wherein the encryption module includes an integrity verification feature in each user key.

45. A system as defined in claim 40, wherein the encryption module includes a checksum in each user key.

46. A system as defined in claim 40, wherein the encryption module includes a message authentication code in each user key.

47. A system as defined in claim 40, wherein the encryption module includes a keyed-hash message authentication code in each user key.

48. A system comprising:

a user key data structure including plurality of user id-user key pairs, each user key pair including a user key and a user id associated with one of a plurality of users, each user key comprising an encrypted version of a common master key;

a master key decryption module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users and to decrypt the selected user key using a password received from the one of the plurality of users.

49. A system as recited in claim 48, further comprising a data decryption module operable to decrypt data encrypted using the master key as an encryption key.

50. A system as recited in claims 48, further comprising an error handler module operable to indicate to the one of the plurality when an error occurs in decrypting the user key.

51. A system as recited in claims 48, wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users to produce a hash value; and

a user key decryption module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users and to decrypt the selected user key using the hash value as a decryption key.

52. A system as recited in claims 48, wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users using a one-way hashing function to produce a hash value; and

a user key decryption module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users and to decrypt the selected user key using the hash value as a decryption key.

53. A system as recited in claim 48, wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users using a cryptographic hashing function to produce a hash value; and

a user key decryption module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users and to decrypt the selected user key using the hash value as a decryption key.

54. A system as recited in claims 48, wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users to produce a hash value; and

a user key decryption and integrity module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users, to confirm the integrity of the selected user id, and to decrypt the selected user key using the hash value as a decryption key.

55. A system as recited in claims 48, wherein each user key in the user key data structure includes an integrity verification feature, and wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users to produce a hash value; and

a user key decryption and integrity module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users, to confirm the integrity of the selected user id using the integrity verification feature included in the user key, and to decrypt the selected user key using the hash value as a decryption key.

56. A system comprising:

means for producing a user key associated with each of a plurality users, each user key comprising a master key encrypted using a password of the one of the plurality of users associated with the user key;

means for associating each of the user keys with a user id of the one of the plurality of users associated with the user key in a data structure.

57. A computer-readable medium having stored thereon computer executable instructions for performing acts of:

creating a data structure including a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key comprising a master key encrypted using a password associated with the one of the plurality of users.

58. A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

delivering the data structure to one or more of the plurality of users.

59. A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

delivering the data structure to each of the plurality of users.

60. A computer-readable medium as recited in claim 57, wherein each master key is encrypted using a hash of the password associated with the one of the plurality of users.

61. A computer-readable medium as recited in claim 57, wherein each master key is encrypted using a one-way hash of the password associated with the one of the plurality of users.

62. A computer-readable medium as recited in claim 57, wherein each master key is encrypted using a cryptographic hash of the password associated with the one of the plurality of users.

63. A computer-readable medium as recited in claim 57, wherein each user key has an integrity verification feature associated therewith.

64 A computer-readable medium as recited in claim 57, wherein each user key includes a checksum.

65. A computer-readable medium as recited in claim 57, wherein each user key includes a keyed-hash message authentication code.

66. A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

transforming data using the master key.

67. A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

storing data transformed using the master key; and

controlling access by the plurality of users to the transformed data.

68. A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

storing data transformed using the master key;

receiving a user id and user password from one of the plurality of users; and

controlling access to the transformed data by the one of the plurality of users based on the received user id and user password.

69. A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

storing data encrypted using the master key;

receiving a user id and user password from one of the plurality of users; and

accessing the transformed data using the received user id and user password.

70. A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

storing data encrypted using the master key;

receiving a user id and user password from one of the plurality of users;

selecting a user key from the data structure based on the received user id;

decrypting the selected user id using the received password to reproduce the master key; and

using the master key to decrypt the data.

71. A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

storing data watermarked using the master key;

receiving a user id and user password from one of the plurality of users; and

selecting a user key from the data structure based on the received user id;

hashing the received password to produce a hash value;

decrypting the selected user id using the hash value to reproduce the master key; and

using the master key to access the watermarked data.

72. A computer-readable medium having stored thereon computer executable instructions for performing acts of:

retrieving a user key associated with a first user of a plurality of users from a data structure comprising a plurality of user keys, each user key comprising a master key encrypted using a password associated with a unique one of the plurality of users;

decrypting the retrieved user key using a password associated with the first user to produce a master key; and

accessing data using the master key.

73. A computer-readable medium as recited in claim 72, wherein the user key is retrieved using a user id associated with the first user.

74. A computer-readable medium as recited in claim 72, wherein the data structure comprises a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key associated with the one of the plurality of users.

75. A computer-readable medium as recited in claim 72, wherein the data structure comprises a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key associated with the one of the plurality of users, and wherein the user key is retrieved using a user id associated with the first user.

76. A computer-readable medium as recited in claim 72, wherein the act of decrypting the user key comprises decrypting the user key using a hash of the password associated with the first user.

77. A computer-readable medium as recited in claim 72, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user to produce a hash value; and

using the hash value as a decryption key to decrypt the user key.

78. A computer-readable medium as recited in claim 72, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user using a one-way hash function; and

using the result of the one-way hash function as a decryption key to decrypt the user key.

79. A computer-readable medium as recited in claim 72, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user using a cryptographic hash function; and

using the result of the cryptographic hash function as a decryption key to decrypt the user key.

80. A computer-readable medium as recited in claim 72, wherein each of the plurality of user key includes a data verification feature.

81. A computer-readable medium as recited in claim 72 having further computer executable instructions for performing acts of:

verifying the integrity of the retrieved user key.

82. A computer-readable medium as recited in claim 72, wherein the retrieved user key includes an integrity verification feature and wherein the

method further comprises verifying the integrity of the retrieved user key using the integrity verification feature.

83. A computer-readable medium as recited in claim 72, wherein the retrieved user key includes a checksum and wherein the method further comprises verifying the integrity of the retrieved user key using the checksum.

84. A computer-readable medium as recited in claim 72, wherein the retrieved user key includes a message authentication code and wherein the method further comprises verifying the integrity of the retrieved user key using the message authentication code.

85. A computer-readable medium as recited in claim 72, wherein the retrieved user key includes a keyed-hash message authentication code and wherein the method further comprises verifying the integrity of the retrieved user key using the keyed-hash message authentication code.